

The mission of the Cyber Vault is to use primary source, policy, and analysis documents to grow a resource for use by researchers, students, instructors, analysts, and government workers. This last category, government workers, has presented complications when one considers the significance of document released through illegal measures. Today the Cyber Vault is taking steps to address this issue.

At the heart of the complication is a set of dueling interests. On the one hand, the Cyber Vault considers leaked documents, when policy-relevant, to be unassailably historically relevant documents. We acknowledge openly that FOIA declassification is the superior avenue of document release for several reasons, not least of which that documents released through FOIA come with a guarantee of authenticity while leaked documents carry differing degrees of validity, however when the leak of certain documents has policy impact then the documents themselves become historically relevant despite a lack of guaranteed authenticity. As such, these documents belong in a store of documents dedicated to the history of cybersecurity policy.

On the other hand, the presence of documents which, if genuine, still carry a secret or top-secret classification is problematic for a set of our intended audience. Government workers are regularly instructed that classified information must be treated as such regardless of public release, which places them in a difficult position when trying to use the Cyber Vault for research.

We believe we have arrived at a solution which satisfies both interests. Documents which carry an active classification have been sorted and are now excluded from Cyber Vault searches by default. Users of the Vault can then opt-in to viewing these documents in their searches.

We are taking an additional step, however. Documents released through the Vault 7 leaks have been removed from the Cyber Vault entirely. These documents are technical, are not related to policy, and may be used to instruct or guide the development of tools for computer network operations. This extends beyond the intended scope of the Cyber Vault. For the sake of historical record we will maintain these documents internally, however we will no longer provide them publicly.

Any questions regarding this decision can be sent to Michael Martelle, the Cyber Vault Research Fellow, and mmartelle@gwu.edu.